UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/851,474	05/08/2001	Timofei Kouzminov	56234-077 (GUZL-152)	3785

7590 05/13/2005

McDermott, Will & Emery
28 State Street
Boston, MA 02109

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/851,474	KOUZMINOV, TIMOFEI	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. An amendment was received on 06 January 2005. No claims have been amended, added, or canceled. Claims 1-15 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 06 January 2005 have been fully considered but they are not persuasive.

Claims 2-4, 7-9, and 13-15 were rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. Applicant argues that the claims and specification do comply with the enablement requirement; however, the Examiner respectfully disagrees. The determination of a failure to comply with the enablement requirement is made considering the undue experimentation factors set forth in MPEP § 2164.01(a). The Examiner believes that, in the instant application, the factor that weighs most heavily is the amount of direction provided by the inventor (see MPEP § 2164.03). The specification merely states, "It will be understood that any type of encryption algorithm may be used to encrypt/decrypt the initial state, as long as the algorithm operates according to the equations 1-3 above" (page 11, lines 1-3). Although MPEP states that "a single embodiment may provide broad enablement in cases involving predictable factors" (2164.03), Applicant's suggestion of "any type of

encryption algorithm" that conforms to the given equations does not provide a specific "single embodiment" as suggested by the MPEP, in light of the state of the prior art. Although Applicant argues that it is not necessary that one decryption operation correspond to one encryption operation, the Examiner again notes that encryption algorithms in general require one decryption operation to correspond to each encryption operation and that such a correspondence of two encryptions to one decryption would be the exception; the Examiner further considers that one of ordinary skill in the art at the time of the invention would similarly take note. Therefore, the Examiner believes that unreasonable experimentation would be required to determine or design such an algorithm because no details have been given in the specification that would allow a person of ordinary skill in the art to perform the specific operations desired by Applicant (see MPEP § 2164.06). The Examiner additionally notes that no specific working example of such an algorithm has been provided in the specification (see MPEP § 2164.02). Therefore, upon consideration of the above factors as a whole, the Examiner maintains that the enablement requirement has not been satisfied and undue experimentation would be required.

Regarding the rejection of Claims 1, 5, 6, and 10-12 under 35 U.S.C. 103(a) as unpatentable over Kessner, "Copy Protection for SRAM based FPGA Designs", in view of Eskicioglu, PCT Publication WO99/30499, Applicant argues that the two references are in different technology fields, that there is no suggestion to combine the references, and that the conclusion that the combination would render the claimed invention obvious is based on hindsight.

In response to applicant's argument that Eskicioglu is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, as Applicant states on pages 2-3 of the present response, Kessner is directed to a technique for copy protection of an FPGA, and Eskicioglu is directed to a method of protecting data from illegal copying. The Examiner therefore believes that the two references are indeed analogous art; namely, both relate to data security, specifically copy protection.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation to combine is as stated in the previous Office action, namely to implement renewable security and to allow for easier and less expensive replacement or upgrade of systems.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon

hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Specifically, Applicant argues that Kessner "lacks the configuration for generating a challenge sequence and further testing the authenticity of the devices"; however, the Examiner notes that Kessner was not relied upon to teach such features and that Eskicioglu was instead relied upon to disclose, for example, further testing authenticity (see Eskicioglu, page 7, line 36-page 8, line 2).

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 2-4, 7-9, and 13-15 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Specifically, Claims 2, 7, and 13 recite that two encryptions are to take place before a decryption. Claims 3, 10, and 14 make clear that it is only one decryption that takes place after the two encryptions. The specification states that "any type of encryption algorithm may be used" as long as the algorithm adheres to the equation recited in Claims 3, 10, and 14 where an original plaintext is recovered after the three operations (see page 11 of Applicant's specification); however, encryption algorithms generally require one decryption operation to correspond to each encryption operation. Thus, it is unclear how one would use such an algorithm to recover a plaintext with two encryptions but only one decryption. The claims are therefore not sufficiently enabled by the disclosure. Note the analysis above in response to Applicant's arguments, specifically detailing the undue experimentation factors considered as per MPEP § 2164.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 5, 6, and 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessner, "Copy Protection for SRAM based FPGA Designs", in view of Eskicioglu, PCT Publication WO99/30499.

In reference to Claim 1, Kessner discloses a system for copy protecting an FPGA including a CPLD that includes a sequence generator and an FPGA that includes a sequence generator and a sequence comparison device. Kessner further discloses that the CPLD initializes its sequence generator, which generates a first sequence based on its initial value, and transmits the first sequence to the FPGA. Kessner also discloses that the FPGA initializes its sequence generator, which generates a second sequence based on its same initial value, and compares the received first sequence with the generated second sequence, and enables operation of the FPGA if the sequences match (see page 2, section "Overview"). However, Kessner does not explicitly disclose how the initial value of the sequence generators is generated; specifically, Kessner does not disclose that an initial state is generated and encrypted in the CPLD, transmitted to the FPGA, and decrypted in the FPGA.

Eskicioglu discloses a method for protecting data that includes generating an initial value (page 6, lines 18-20, where the key is the initial value, as stated at page 6, lines 11-12) and encrypting and sending the initial value to a receiver (page 6, lines 24-31). Eskicioglu further discloses that the received initial value is decrypted (page 6, lines 31-33) and that the initial value is used as a seed to generate a sequence in both the transmitter and the receiver (page 3, lines 16-32, and Figure 2, where the keystream

is the generated sequence). Eskicioglu also discloses the use of a challenge sequence provided to the sequence generators (page 7, line 5-page 8, line 31, where additional inputs are used in generating the keystream sequences).

Therefore, it would have been obvious to one of ordinary skill in the art to modify the system of Kessner by sending an encrypted initial value, decrypting the received initial value, and using the decrypted initial value in generating the sequences, in order to implement renewable security to allow for the development of systems that can be replaced or upgraded more easily and with less expense (see Eskicioglu, page 1, lines 28-30).

Claims 5 and 6 contain all the limitations of Claim 1, and are therefore rejected by a similar rationale.

Claims 10 and 11 are method claims corresponding substantially to the systems of Claims 5 and 6, respectively, and are rejected by a similar rationale.

In reference to Claim 12, Eskicioglu further discloses encrypting the initial state with a key (page 6, lines 24-31).

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER